| Zuständigkeiten | Rollen |
|---|---|
| Grundsätzlich zuständig | IT-Betrieb |
| Weitere Zuständigkeiten | Testende, Fachverantwortliche, Datenschutzbeauftragte, Personalabteilung |

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

## 3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

### OPS.1.1.6.A1 Planung der Software-Tests (B)

Die Rahmenbedingungen für Software-Tests MÜSSEN vor den Tests innerhalb der Institution entsprechend der Schutzbedarfe, Organisationseinheiten, technischen Möglichkeiten und Test-Umgebungen festlegt sein. Die Software MUSS auf Basis der Anforderungen des Anforderungskatalogs zu der Software getestet werden. Liegt auch ein Pflichtenheft vor, dann MUSS dieses zusätzlich berücksichtigt werden.

Die Testfälle MÜSSEN so ausgewählt werden, sodass diese möglichst repräsentativ alle Funktionen der Software überprüfen. Zusätzlich SOLLTEN auch Negativ-Tests berücksichtigt werden, die überprüfen, ob die Software keine ungewollten Funktionen enthält.

Die Testumgebung MUSS so ausgewählt werden, sodass diese möglichst repräsentativ alle in der Institution eingesetzten Gerätemodelle und Betriebssystemumgebungen abdeckt. Es SOLLTE dabei getestet werden, ob die Software mit den eingesetzten Betriebssystemen in den vorliegenden Konfigurationen kompatibel und funktionsfähig ist.

### OPS.1.1.6.A2 Durchführung von funktionalen Software-Tests (B) [Testende]

Mit funktionalen Software-Tests MUSS die ordnungsgemäße und vollständige Funktion der Software überprüft werden. Die funktionalen Software-Tests MÜSSEN so durchgeführt werden, dass sie den Produktivbetrieb nicht beeinflussen.

### OPS.1.1.6.A3 Auswertung der Testergebnisse (B) [Testende]

Die Ergebnisse der Software-Tests MÜSSEN ausgewertet werden. Es SOLLTE ein Soll-Ist-Vergleich mit definierten Vorgaben durchgeführt werden. Die Auswertung MUSS dokumentiert werden.

### OPS.1.1.6.A4 Freigabe der Software (B) [Fachverantwortliche]

Die fachlich zuständige Organisationseinheit MUSS die Software freigeben, sobald die Software-Tests erfolgreich durchgeführt wurden. Die Freigabe MUSS in Form einer Freigabeerklärung dokumentiert werden.

Die freigebende Organisationseinheit MUSS überprüfen, ob die Software gemäß den Anforderungen getestet wurde. Die Ergebnisse der Software-Tests MÜSSEN mit den vorher festgelegten Erwartungen übereinstimmen. Auch MUSS überprüft werden, ob die rechtlichen und organisatorischen Vorgaben eingehalten wurden.

### OPS.1.1.6.A5 Durchführung von Software-Tests für nicht funktionale Anforderungen (B) [Testende]

Es MÜSSEN Software-Tests durchgeführt werden, die überprüfen, ob alle wesentlichen nichtfunktionalen Anforderungen erfüllt werden. Insbesondere MÜSSEN sicherheitsspezifische Software-Tests durchgeführt werden, wenn die Anwendung sicherheitskritische Funktionen mitbringt. Die durchgeführten Testfälle, sowie die Testergebnisse, MÜSSEN dokumentiert werden.

### OPS.1.1.6.A11 Verwendung von anonymisierten oder pseudonymisierten Testdaten (B) [Datenschutzbeauftragte, Testende]

Wenn Produktivdaten für Software-Tests verwendet werden, die schützenswerte Informationen enthalten, dann MÜSSEN diese Testdaten angemessen geschützt werden. Enthalten diese Daten personenbezogene Informationen, dann MÜSSEN diese Daten mindestens pseudonymisiert werden. Falls möglich, SOLLTEN die Testdaten mit Perso-

nenbezug vollständig anonymisiert werden. Wenn ein Personenbezug von den Testdaten abgeleitet werden könnte, MUSS der oder die Datenschutzbeauftragte und unter Umständen die Personalvertretung hinzugezogen werden.

## 3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

**OPS.1.1.6.A6 Geordnete Einweisung der Software-Testenden (S) [Fachverantwortliche]**

Die Software-Testenden SOLLTEN über die durchzuführenden Testarten und die zu testenden Bereiche einer Software von Fachverantwortlichen informiert werden. Darüber hinaus SOLLTEN die Software-Testende über die Anwendungsfälle und mögliche weitere Anforderungen der Software informiert werden.

**OPS.1.1.6.A7 Personalauswahl der Software-Testenden (S) [Personalabteilung, Fachverantwortliche]**

Bei der Auswahl der Software-Testenden SOLLTEN gesonderte Auswahlkriterien berücksichtigt werden. Die Software-Testenden SOLLTEN die erforderliche berufliche Qualifikation haben.

Wird Individualsoftware auf Quellcode-Ebene überprüft, dann SOLLTEN die Testenden über ausreichendes Fachwissen über die zu testenden Programmiersprache und der Entwicklungsumgebung verfügen. Der Quellcode SOLLTE NICHT ausschließlich von Testenden überprüft werden, die auch an der Erstellung des Quellcodes beteiligt waren.

**OPS.1.1.6.A8 ENTFALLEN (S)**

Diese Anforderung ist entfallen.

**OPS.1.1.6.A9 ENTFALLEN (S)**

Diese Anforderung ist entfallen.

**OPS.1.1.6.A10 Erstellung eines Abnahmeplans (S)**

In einem Abnahmeplan SOLLTEN die durchzuführenden Testarten, Testfälle und die erwarteten Ergebnisse dokumentiert sein. Außerdem SOLLTE der Abnahmeplan die Freigabekriterien beinhalten. Es SOLLTE eine Vorgehensweise für die Situation festgelegt werden, wenn eine Freigabe abgelehnt wird.

**OPS.1.1.6.A12 Durchführung von Regressionstests (S) [Testende]**

Wenn Software verändert wurde, SOLLTEN Regressionstests durchgeführt werden. Hierbei SOLLTE überprüft werden, ob bisherige bestehende Sicherheitsmechanismen und -einstellungen durch das Update ungewollt verändert wurden. Regressionstests SOLLTEN vollständig durchgeführt werden und hierbei auch Erweiterungen sowie Hilfsmittel umfassen. Werden Testfälle ausgelassen, SOLLTE dies begründet und dokumentiert werden. Die durchgeführten Testfälle und die Testergebnisse SOLLTEN dokumentiert werden.

**OPS.1.1.6.A13 Trennung der Testumgebung von der Produktivumgebung (S)**

Software SOLLTE nur in einer hierfür vorgesehenen Testumgebung getestet werden. Die Testumgebung SOLLTE von der Produktivumgebung getrennt betrieben werden. Die in der Testumgebung verwendeten Architekturen und Mechanismen SOLLTEN dokumentiert werden. Es SOLLTEN Verfahren dokumentiert werden, wie mit der Testumgebung nach Abschluss des Software-Tests zu verfahren ist.

**OPS.1.1.6.A15 Überprüfung der Installation und zugehörigen Dokumentation (S) [Testende]**

Die Installation der Software SOLLTE entsprechend der Regelungen zur Installation und Konfiguration von Software (siehe Baustein APP.6 *Allgemeine Software*) überprüft werden. Falls vorhanden, SOLLTE zusätzlich die Installations- und Konfigurationsdokumentation geprüft werden.

## 3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

**OPS.1.1.6.A14 Durchführung von Penetrationstests (H) [Testende]**

Für Anwendungen beziehungsweise IT-Systeme mit erhöhtem Schutzbedarf SOLLTEN Penetrationstests als Testmethode durchgeführt werden. Ein Konzept für Penetrationstests SOLLTE erstellt werden. Im Konzept für Penetrationstests SOLLTEN neben den zu verwendenden Testmethoden auch die Erfolgskriterien dokumentiert werden.

Der Penetrationstest SOLLTE nach den Rahmenbedingungen des Penetrationstest-Konzepts erfolgen. Die durch den Penetrationstest aufgefundenen Sicherheitslücken SOLLTEN klassifiziert und dokumentiert sein.

**OPS.1.1.6.A16 Sicherheitsüberprüfung der Testenden (H)**

Sofern Testende auf besonders schützenswerte Informationen zugreifen müssen, SOLLTE die Institution Nachweise über ihre Integrität und Reputation einholen. Handelt es sich dabei um klassifizierte Verschlusssachen, SOLLTEN sich die Software-Testenden einer Sicherheitsüberprüfung nach dem Sicherheitsüberprüfungsgesetz (SÜG) unterziehen. Hierzu SOLLTE der oder die ISB die Geheimschutzbeauftragten bzw. Sicherheitsbevollmächtigten der Institution einbeziehen.

# 4. Weiterführende Informationen

## 4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 im Annex A.14 „System Acquisition, Development and maintenance" Anforderungen an die sichere System-Entwicklung, die auch einen Test- und Freigabeprozess erfordert, sowie direkt an Testdaten selbst. Darüber hinaus hat die ISO die Norm ISO/IEC 29119-2:2013 „Software and systems engineering – Software testing – Part 2: Test processes, International Organization for Standardization" veröffentlicht, die ausführlich Anforderungen an Software-Tests behandelt.

Das BSI hat die Studie „Durchführungskonzept für Penetrationstests", die als Grundlage für Penetrationstests verwendet werden kann, sowie den BSI-Leitfäden zur Entwicklung sicherer Webanwendungen, der auch Software-Tests inkludiert, veröffentlicht.

Das Information Security Forum (ISF) führt in „The Standard of Good Practice for Information Security" Aspekte zum Testen und Freigeben zu allen relevanten Anforderungen (Areas) aus.

Das National Institute of Standards and Technology stellt Richtlinien zum Testen von Software in der NIST Publication 800-53 in der SA 11 Developer Security Testing and Evaluation zur Verfügung.

Das Buch „The Art of Software Testing" von Glenford J. Myers, Corey Sandler, Tom Badgett, kann für Software-Tests konsultiert werden.

Das Common Vulnerability Scoring System kann als Scoring-System zur Klassifikation des Schweregrades einer Sicherheitslücke verwendet werden und somit die Ergebnisse von Software-Tests in Bezug auf die Informationssicherheit darstellen.

Bundesamt
für Sicherheit in der
Informationstechnik

# OPS.1.1.7 Systemmanagement

## 1. Beschreibung

### 1.1. Einleitung

Ein zuverlässiges Systemmanagement ist Grundvoraussetzung für den sicheren und effizienten Betrieb moderner vernetzter Systeme. Dazu ist es erforderlich, dass ein Systemmanagement alle relevanten Systeme umfassend integriert. Außerdem müssen geeignete Maßnahmen umgesetzt werden, um die Systemmanagement-Kommunikation und -infrastruktur zu schützen.

Das Systemmanagement umfasst viele wichtige Funktionen wie z. B. die Systemüberwachung, die Konfiguration der Systeme, die Behandlung von Ereignissen und die Protokollierung. Eine weitere wichtige Funktion ist das Reporting, das auch als gemeinsame Plattform für IT-Systeme und Netzkomponenten angelegt werden kann. Alternativ kann es dediziert als einheitliche Plattform oder als Bestandteil der einzelnen Systemmanagement-Komponenten realisiert werden.

Die Systemmanagement-Lösung besteht aus verschiedenen Systemmanagement-Komponenten, zum Beispiel Agenten, die auf einer zugrundeliegenden Systemmanagement-Infrastruktur betrieben werden. Diese Lösung wird genutzt, um die eingebundenen und zu verwaltenden Systeme über die entsprechenden Schnittstellen des Informationsverbundes zu steuern. Die Kombination aus der Lösung, der zugrundeliegenden Infrastruktur, den zu verwaltenden Systemen und dem Betrieb bildet die Gesamtheit des Systemmanagements.

### 1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil des Systemmanagements zu etablieren. Der Baustein beschreibt zum einen, wie das Systemmanagement aufgebaut und abgesichert werden kann, und zum anderen, wie die zugehörige Kommunikation geschützt werden kann.

### 1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.1.7 *Systemmanagement* ist auf die Systemmanagement-Lösung anzuwenden, die im Informationsverbund eingesetzt wird.

Um ein IT-Grundschutz-Modell für einen konkreten Informationsverbund zu erstellen, muss grundsätzlich die Gesamtheit aller Bausteine betrachtet werden. In der Regel sind mehrere Bausteine auf das Thema bzw. Zielobjekt anzuwenden.

Dieser Baustein behandelt z. B.

- die notwendigen Systemmanagement-Komponenten,
- die konzeptionellen Aufgaben zum Systemmanagement,
- Protokollierung unter dem Gesichtspunkt des Systemmanagements sowie
- die Aktualisierung der Systemmanagement-Lösung.

Folgende Inhalte sind ebenfalls von Bedeutung und werden an anderer Stelle behandelt:

- Anforderungen zum Netzmanagement (siehe NET.1.2 *Netzmanagement)*
- Details bezüglich der Absicherung der zugrundeliegenden Infrastruktur und von zu verwaltenden IT-Systemen, insbesondere deren Management-Schnittstellen (siehe SYS.2 *IT-Systeme)*
- Protokollierungs- und Archivierungskonzepte (siehe OPS.1.1.5 *Protokollierung*, OPS.1.2.2 *Archivierung*)

- Aktualisierung z. B. durch Zusatzsoftware, sogenannte Agenten (siehe OPS.1.1.3 *Patch- und Änderungsmanagement*)
- Zugriffe von Benutzenden auf die Systemmanagement-Lösung (siehe ORP.4 *Identitäts- und Berechtigungsmanagement*, sowie OPS.1.2.5 *Fernwartung* und OPS.1.1.2 *Ordnungsgemäße IT-Administration*).

# 2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.1.7 *Systemmanagement* von besonderer Bedeutung.

## 2.1. Unberechtigter Zugriff auf die Systemmanagement-Lösung

Das Systemmanagement ist aufgrund seiner zentralen Stellung und aufgrund der notwendigen Zugriffsrechte auf alle zu verwaltenden Systeme ein vorrangiges Ziel für Angriffe.

Wenn es Angreifenden gelingt auf Systemmanagement-Lösungen zuzugreifen, z. B. durch ungepatchte Sicherheitslücken, dann können diese alle vom Systemmanagement verwalteten Systeme kontrollieren und neu konfigurieren. So können sie z. B. auf schützenswerte Informationen zugreifen oder auch Dienste oder verwaltete Systeme stören. Beispielsweise könnte ein Unternehmen zentral Konfigurationsserver für eine Systemmanagementlösung bereitstellen. Über eine ungepatchte Schwachstelle werden in diesem Beispiel die Konfigurationsdateien so verändert, dass die verwalteten Systeme eine Ransomware installieren. In Folge werden in diesem Beispiel alle Systeme, die von dieser Systemmanagementlösung verwaltet werden, verschlüsselt.

## 2.2. Fehler in Automatisierungsfunktionen für das Systemmanagement

Alle Schutzziele des zu verwaltenden Informationssysteme können durch fehlerhaft automatisierte Abläufe beeinträchtigt sein.

Durch Fehler in einer oder mehreren Automatisierungsfunktionen wie z. B. Skripte, können die zu verwaltenden Systeme funktionsunfähig oder kompromittiert werden. Wegen der automatisierten Abläufe kann schnell eine große Anzahl von IT-Systemen kompromittiert werden. Auch besonders kritische IT-Systeme können auf diesem Weg schnell kompromittiert werden.

## 2.3. Unberechtigte Eingriffe in die Systemmanagement-Kommunikation

Versehentliche Eingriffe in oder gezielte Angriffe auf die Kommunikation des Systemmanagements können die Integrität der verwalteten IT-Systeme verletzen und die Verfügbarkeit von Diensten oder IT-Systemen einschränken.

Wird die Systemmanagement-Kommunikation abgehört und manipuliert, dann können auf diesem Weg aktive Systeme kontrolliert werden. Außerdem können die von und zu den Systemen übertragenen Daten mitgeschnitten und eingesehen werden.

## 2.4. Unzureichende Zeitsynchronisation der Systemmanagement-Komponenten

Fehler in der Zeitsynchronisation können Probleme und Ereignisse verdecken, sodass z. B. die Erkennung von Sicherheitsvorfällen und Datenabflüssen erschwert wird.

Wenn die Systemzeit der Systemmanagement-Komponenten unzureichend synchronisiert wird, dann können (beispielsweise) Protokolle, die unter anderem Zeitstempel zur Evaluierung der Kommunikationsgültigkeit verwenden, durch unterschiedliche Systemzeiten auf den Systemmanagement-Komponenten und den zu verwaltenden Systemen gestört werden.

Zusätzlich können die Protokollierungsdaten zum Systemmanagement unter Umständen eventuell nicht miteinander korreliert werden. Auch kann die Korrelation eventuell zu fehlerhaften Aussagen führen, wenn Zeitstempel aufgrund fehlerhafter Synchronisation nur scheinbar übereinstimmen oder abweichen.

### 2.5. Inkompatibilität zwischen den zu verwaltenden Systemen und der Systemmanagement-Lösung

Eine nur unvollständig kompatible Systemmanagement-Lösung kann Fehlfunktionen der zu verwaltenden IT-Systeme auslösen und deren Verfügbarkeit einschränken.

Falls die Systemmanagement-Lösung die zu verwaltenden IT-Systeme nicht vollständig unterstützt, können bestimmte Aktionen nicht wie geplant durchgeführt werden. Diese Gefährdung kann auch bei einer Aktualisierung der Systeme auftreten, bei der die Management-Schnittstellen verändert werden.

### 2.6. Verbindungsverlust zwischen Anwendenden und Systemmanagement-Lösung

Verbindungsabbrüche können die Verfügbarkeit der Systemmanagement-Lösung einschränken.

Wenn die Verbindung zwischen den Administrierenden und der Systemmanagement-Lösung gestört wird, können IT-Systeme ausfallen. Außerdem können eine Fehlerbehebung und die Verwaltung von IT-Systemen erschwert werden.

Wenn eine Verbindung abbricht oder gestört wird, dann können kostenintensive sicherheitsrelevante sowie zeitkritische Arbeiten nicht fristgerecht durchgeführt werden, beispielsweise können Sicherheitsupdates nicht mehr eingespielt werden oder auf Sicherheitsvorfälle nicht angemessen reagiert werden.

### 2.7. Verbindungsverlust zwischen Systemmanagement-Lösung und zu verwaltenden Systemen

Verbindungsabbrüche zu den zu verwaltenden Systemen können insbesondere die Verfügbarkeit oder Integrität von Diensten im Informationsverbund beeinträchtigen.

Der Umfang und die Konstellation eines solchen Verbindungsverlusts entscheiden darüber, ob Dienste beeinträchtigt werden und welche Schäden entstehen können. Die resultierenden Fehlerbilder sind unter Umständen schwer zu analysieren und die auftretenden Fehler schwer zu beheben.

### 2.8. Unzureichende Abstimmung zwischen Systemmanagement und Netzmanagement

Nicht abgestimmte Aktionen im Netzmanagement können sich negativ auf das Systemmanagement auswirken. Dadurch können Inkonsistenzen in der Konfiguration zwischen IT-Systemen und verbindenden Netzen entstehen. So können z. B. Verbindungsverluste im Netz eine große Anzahl von Folgeereignissen im Bereich Systemmanagement auslösen. Diese Ereignisse können bis zu Fehlkonfigurationen reichen.

## 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.1.7 *Systemmanagement* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

| Zuständigkeiten | Rollen |
|---|---|
| Grundsätzlich zuständig | IT-Betrieb |
| Weitere Zuständigkeiten | Keine |

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

## 3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

### OPS.1.1.7.A1 Anforderungsspezifikation für das Systemmanagement (B)

Anforderungen an die Systemmanagement-Infrastruktur und -Prozesse MÜSSEN spezifiziert werden. Dabei MÜSSEN alle wesentlichen Elemente für das Systemmanagement berücksichtigt werden. Auch MÜSSEN die Sicherheitsaspekte für das Systemmanagement von Beginn an beachtet werden.

Zudem MÜSSEN die Schnittstellen der zu verwaltenden IT-Systeme dokumentiert werden, z. B. um die Kompatibilität von Systemmanagement-Lösung und zu verwaltendem System zu gewährleisten.

### OPS.1.1.7.A2 Planung des Systemmanagements (B)

Die Systemmanagement-Lösung und die zugrundeliegende Infrastruktur MÜSSEN geeignet geplant werden. Die Planung MUSS mindestens die folgenden Inhalte umfassen:

- eine detaillierte Anforderungsanalyse,
- ein aussagekräftiges Grobkonzept,
- einen umfassenden Umsetzungsplan sowie
- Meilensteine für Qualitätssicherung und Abnahme.

Dabei MÜSSEN alle in der Anforderungsspezifikation genannten Punkte sowie das Rollen- und Berechtigungskonzept berücksichtigt werden. Es MÜSSEN mindestens die folgenden Themen berücksichtigt werden:

- Trennung in geeignete Bereiche für das Systemmanagement,
- Zugriffsmöglichkeiten auf und durch das Systemmanagement,
- Berechtigungen des Systemmanagements auf den zu verwaltenden Systemen,
- Netzverbindungen für den Zugriff auf und durch das Systemmanagement,
- Protokolle für den Zugriff von Benutzenden auf die Systemmanagement-Lösung,
- Protokolle für die Kommunikation zwischen der Systemmanagement-Lösung und den zu verwaltenden Systemen,
- Anforderungen an Systemmanagement-Werkzeuge,
- Schnittstellen, um erfasste Ereignis- oder Alarmmeldungen weiterzuleiten,
- Protokollierung, inklusive erforderlicher Schnittstellen zu einer zentralen Protokollierungslösung,
- Unterstützung durch das herstellende bzw. entwickelnde Unternehmen über den geplanten Einsatzzeitraum,
- Möglichkeiten zum Einspielen von Patches für die Systemmanagement-Lösung sowie für die zu verwaltenden Systeme,
- Reporting und Schnittstellen zu übergreifenden Lösungen sowie
- korrespondierende Anforderungen an die zu verwaltenden Systeme.

### OPS.1.1.7.A3 Zeitsynchronisation für das Systemmanagement (B)

Alle Komponenten der Systemmanagement-Lösung, inklusive der zu verwaltenden Systeme, MÜSSEN eine synchrone Uhrzeit nutzen. Die Systemzeit MUSS für jedes zu verwaltende System und für die Systemmanagement-Lösung über geeignete Protokolle synchronisiert werden.

### OPS.1.1.7.A4 Absicherung der Systemmanagement-Kommunikation (B)

Sobald die Systemmanagement-Lösung und die zu verwaltenden Systeme über die produktive Infrastruktur kommunizieren, MÜSSEN dafür sichere Protokolle verwendet werden. Falls keine sicheren Protokolle verwendet werden können, dann MUSS ein eigens dafür vorgesehenes Administrationsnetz (Out-of-Band-Management) verwendet werden (siehe NET.1.1 *Netzarchitektur und -design*). Ist auch dies nicht möglich, dann MÜSSEN ergänzende Sicherheitsmechanismen auf anderer Ebene eingesetzt werden, z. B. Tunnelmechanismen über verschlüsseltes VPN oder vergleichbare Lösungen.

**OPS.1.1.7.A5 Gegenseitige Authentisierung von Systemmanagement-Lösung und zu verwaltenden Systemen (B)**

Die Authentisierung zwischen Systemmanagement-Lösung und zu verwaltenden Systemen MUSS in beide Richtungen erfolgen. Die Authentisierung MUSS in das übergreifende Authentisierungskonzept eingebunden sein. Die Authentisierung MUSS mittels sicherer Protokolle erfolgen.

**OPS.1.1.7.A6 Absicherung des Zugriffs auf die Systemmanagement-Lösung (B)**

Der Zugriff von Benutzenden auf die Systemmanagement-Lösung MUSS abgesichert werden durch

- eine sichere und angemessene Authentisierung und Autorisierung der Benutzenden sowie
- eine sichere Verschlüsselung der übertragenen Daten.

Eine angemessene Authentisierungsmethode MUSS ausgewählt werden. Der Auswahlprozess MUSS dokumentiert werden. Die Stärke der verwendeten kryptografischen Verfahren und Schlüssel MUSS regelmäßig überprüft und bei Bedarf angepasst werden.

Die Systemmanagement-Lösung MUSS über eine Autorisierungskomponente sicherstellen, dass Benutzende ausschließlich solche Aktionen durchführen können, zu denen sie berechtigt sind.

## 3.2. Standard-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

**OPS.1.1.7.A7 Festlegung einer Sicherheitsrichtlinie für das Systemmanagement (S)**

Für das Systemmanagement SOLLTE eine Sicherheitsrichtlinie erstellt und nachhaltig gepflegt werden. Die Richtlinie SOLLTE allen Personen, die am Systemmanagement beteiligt sind, bekannt sein. Die Sicherheitsrichtlinie SOLLTE zudem grundlegend für die Arbeit dieser Personen sein. Es SOLLTE regelmäßig und nachvollziehbar überprüft werden, dass die in der Richtlinie geforderten Inhalte umgesetzt werden. Die Ergebnisse SOLLTEN dokumentiert werden.

Die Sicherheitsrichtlinie SOLLTE mindestens das Folgende festlegen:

- die Bereiche des Systemmanagements, die über zentrale Management-Werkzeuge und -Dienste realisiert werden,
- die Aufgaben im Systemmanagement, die automatisiert realisiert werden sollen,
- das Konfigurationsmanagement für die Daten, die von der Systemmanagement-Lösung verwaltet werden, z. B. Versionierung von Konfigurationen,
- Vorgaben für die Netztrennung,
- Vorgaben für die Zugriffskontrolle,
- Vorgaben für die Protokollierung,
- Vorgaben für die Qualitätssicherung beim Einsatz von Automatisierungsfunktionen, z. B. Skripte,
- Vorgaben für den Schutz der Kommunikation,
- die operativen Grundregeln des Systemmanagements sowie
- Vorgaben für die Abstimmung mit dem Netzmanagement, z. B. Vergabe von IP-Adressen oder DNS-Namen.

**OPS.1.1.7.A8 Erstellung eines Systemmanagement-Konzepts (S)**

Ausgehend von der Sicherheitsrichtlinie für das Systemmanagement SOLLTE ein Systemmanagement-Konzept erstellt und kontinuierlich gepflegt werden. Dabei SOLLTEN mindestens folgende Aspekte bedarfsgerecht berücksichtigt werden:

- Methoden, Techniken und Werkzeuge für das Systemmanagement,
- Absicherung des Zugangs und der Kommunikation,
- Absicherung auf Ebene des Netzes, insbesondere Zuordnung von Systemmanagement-Komponenten zu Sicherheitszonen,

- Umfang des Monitorings und der Alarmierung für jedes zu verwaltende System,
- Protokollierung,
- Automatisierung, insbesondere die zentrale Verteilung von Konfigurationsdateien auf die zu verwaltenden Systeme,
- Vorgaben an Entwicklung und Test von Automatisierungsfunktionen,
- Meldeketten bei Störungen und Sicherheitsvorfällen,
- Bereitstellung von Systemmanagement-Informationen für andere Betriebsbereiche,
- Einbindung des Systemmanagements in die Notfallplanung, sowie
- benötigten Netzübertragungskapazitäten der Systemmanagement-Lösung.

**OPS.1.1.7.A9 Fein- und Umsetzungsplanung für das Systemmanagement (S)**

Eine Fein- und Umsetzungsplanung für die Systemmanagement-Lösung SOLLTE erstellt werden. Dabei SOLLTEN alle in der Sicherheitsrichtlinie und im Systemmanagement-Konzept adressierten Punkte berücksichtigt werden.

**OPS.1.1.7.A10 Konzept für den sicheren Betrieb der Systemmanagement-Lösung (S)**

Ausgehend von den Sicherheitsrichtlinien und dem Systemmanagement-Konzept SOLLTE ein Konzept für den sicheren Betrieb der Systemmanagement-Lösung und der zugrundeliegenden Infrastruktur erstellt werden.

Auch SOLLTE geprüft werden, wie sich die Leistungen anderer operativer Einheiten einbinden und steuern lassen.

**OPS.1.1.7.A11 Regelmäßiger Soll-Ist-Vergleich im Rahmen des Systemmanagements (S)**

Der IT-Betrieb SOLLTE regelmäßig überprüfen, inwieweit die von der Systemmanagement-Lösung verwalteten Daten, Konfigurationen und Skripte dem Sollzustand entsprechen. Mindestens folgende Aspekte SOLLTEN im Soll-Ist-Vergleich geprüft werden:

- die Konfiguration der Systemmanagement-Lösung,
- die Konfiguration der zu verwaltenden Systeme sowie
- die eingesetzten Automatisierungsfunktionen oder Skripte.

Dabei SOLLTE geprüft werden, ob die genannten Aspekte noch die Sicherheitsrichtlinie und Anforderungsspezifikation erfüllen. Weiter SOLLTE verglichen werden, ob die Softwareversion der Systemmanagement-Lösung aktuell ist.

**OPS.1.1.7.A12 Auslösung von Aktionen durch die zentralen Komponenten der Systemmanagement-Lösung (S)**

Aktionen, die durch das Systemmanagement auf den verwalteten Systemen ausgeführt werden, SOLLTEN ausschließlich von der Systemmanagement-Lösung ausgelöst werden. Dafür SOLLTEN nur diejenigen Management-Funktionen auf der Systemmanagement-Lösung und den zu verwaltenden Systemen aktiviert werden, die tatsächlich benötigt werden.

**OPS.1.1.7.A13 Verpflichtung zur Nutzung der vorgesehenen Schnittstellen für das Systemmanagement (S)**

Management-Zugriffe auf zu verwaltende Systeme SOLLTEN ausschließlich über die dafür vorgesehenen Schnittstellen der Systemmanagement-Lösung erfolgen. Falls ein direkter Zugriff auf zu verwaltende Systeme notwendig ist, z. B. nach einem Ausfall eines zu verwaltenden Systems, SOLLTEN sowohl der direkte Zugriff als auch alle in diesem Rahmen vorgenommenen Änderungen dokumentiert und im notwendigen Umfang in die Systemmanagement-Lösung eingepflegt werden.

**OPS.1.1.7.A14 Zentrale Konfigurationsverwaltung für zu verwaltende Systeme (S)**

Software und Konfigurationsdaten für die zu verwaltenden Systeme SOLLTEN konsequent in einem Konfigurationsmanagement verwaltet werden, das eine Versionierung und Änderungsverfolgung ermöglicht. Die zugehörige Dokumentation zur Konfigurationsverwaltung SOLLTE vollständig und immer aktuell sein. Die benötigten Dokumentationen SOLLTEN an zentraler Stelle sicher verfügbar sein sowie in die Datensicherung eingebunden werden. Die zentrale Konfigurationsverwaltung SOLLTE nachhaltig gepflegt und regelmäßig auditiert werden.

Sämtliche Schnittstellen zwischen Systemmanagement-Lösung und anderen Anwendungen und Diensten SOLLTEN dokumentiert und vollständig in einem Konfigurationsmanagement verwaltet werden. Zwischen relevanten Betriebsbereichen SOLLTEN funktionale Änderungen an den Schnittstellen frühzeitig abgestimmt und dokumentiert werden.

Die Konfigurationsdaten für die zu verwaltenden Systeme SOLLTEN automatisch über das Netz verteilt und ohne Betriebsunterbrechung installiert und aktiviert werden können.

**OPS.1.1.7.A15 Statusüberwachung, Protokollierung und Alarmierung bei relevanten Ereignissen im Systemmanagement-Lösung und den zu verwaltenden Systemen (S)**

Die grundlegenden Performance- und Verfügbarkeitsparameter der Systemmanagement-Lösung und der zu verwaltenden Systeme SOLLTEN kontinuierlich überwacht werden. Dafür SOLLTEN vorab die jeweiligen Schwellwerte ermittelt werden (Baselining). Werden definierte Schwellwerte überschritten, SOLLTE das zuständige Personal automatisch benachrichtigt werden.

Zur besseren Fehleranalyse SOLLTEN Informationen aus der Statusüberwachung anderer Bereiche, z. B. aus einem eigenen Bereich „Netze", ebenfalls betrachtet werden, um die genaue Ursache für eine Störung zu finden.

Wichtige Ereignisse auf zu verwaltenden Systemen und auf der Systemmanagement-Lösung SOLLTEN automatisch an eine zentrale Protokollierungsinfrastruktur übermittelt und dort protokolliert werden (siehe OPS.1.1.5 *Protokollierung*).

Wichtige Ereignisse SOLLTEN mindestens für folgende Aspekte definiert werden:

- Ausfall sowie Nichterreichbarkeit von zu verwaltenden Systemen,
- Ausfall sowie Nichterreichbarkeit von Systemmanagement-Komponenten,
- Hardware-Fehlfunktionen,
- Anmeldeversuche an der Systemmanagement-Lösung,
- Anmeldeversuche an zu verwaltenden Systemen,
- kritische Zustände oder Überlastung der Systemmanagement-Lösung sowie
- kritische Zustände oder Überlastung von zu verwaltenden Systemen.

Ereignismeldungen sowie Protokollierungs-Daten SOLLTEN an ein zentrales Logging-System übermittelt werden. Alarmmeldungen SOLLTEN sofort, wenn sie auftreten, übermittelt werden.

**OPS.1.1.7.A16 Einbindung des Systemmanagements in die Notfallplanung (S)**

Die Systemmanagement-Lösung SOLLTE in die Notfallplanung der Institution eingebunden werden. Dazu SOLLTEN sowohl die Systemmanagement-Lösung als auch die Konfigurationen der zu verwaltenden Systeme gesichert und in die Wiederanlaufpläne integriert sein.

**OPS.1.1.7.A17 Kontrolle der Systemmanagement-Kommunikation (S)**

Die Kommunikation zwischen den Benutzenden und der Systemmanagement-Lösung sowie zwischen der Systemmanagement-Lösung und den zu verwaltenden IT-Systemen SOLLTE über geeignete Filtertechniken auf unbedingt notwendige Verbindungen eingeschränkt werden.

**OPS.1.1.7.A18 Überprüfung des Systemzustands (S)**

Die Konsistenz zwischen realem Systemzustand und dem von der Systemmanagement-Lösung angenommenen Zustand SOLLTE regelmäßig geprüft werden. Werden Abweichungen festgestellt, SOLLTE der in der Systemmanagement-Lösung vorgesehene Zustand wiederhergestellt werden.

**OPS.1.1.7.A19 Absicherung der Systemmanagement-Kommunikation zwischen der Systemmanagement-Lösung und den zu verwaltenden Systemen (S)**

Die Systemmanagement-Kommunikation zwischen der Systemmanagement-Lösung und den zu verwaltenden Systemen SOLLTE grundsätzlich verschlüsselt sein. Die Stärke der verwendeten kryptografischen Verfahren und Schlüssel SOLLTE regelmäßig überprüft und bei Bedarf angepasst werden.

## 3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

**OPS.1.1.7.A20 Hochverfügbare Realisierung der Systemmanagement-Lösung (H)**

Eine zentrale Systemmanagement-Lösung SOLLTE hochverfügbar betrieben werden. Dazu SOLLTEN die für die Systemmanagement-Lösung eingesetzten Server bzw. Werkzeuge inklusive der Netzanbindungen redundant ausgelegt sein.

**OPS.1.1.7.A21 Physische Trennung der zentralen Systemmanagementnetze (H)**

Das Managementnetz für das Systemmanagement SOLLTE physisch von den funktionalen, insbesondere produktiven, Netzen getrennt werden.

**OPS.1.1.7.A22 Einbindung des Systemmanagements in automatisierte Detektionssysteme (H)**

Die Protokollierung von sicherheitsrelevanten Ereignissen des Systemmanagements SOLLTE in ein Security Information and Event Management (SIEM) eingebunden werden. Dabei SOLLTE nachvollziehbar festgelegt werden, welche Ereignisse an das SIEM weitergeleitet werden.

Im Anforderungskatalog zur Auswahl einer Systemmanagement-Lösung SOLLTEN die erforderlichen Schnittstellen und Übergabeformate spezifiziert werden.

Eine Systemmanagement-Lösung SOLLTE mit einem System zur Erkennung sicherheitsrelevanter Schwachstellen automatisiert überwacht werden.

**OPS.1.1.7.A23 Standort-übergreifende Zeitsynchronisation für das Systemmanagement (H)**

Die Zeitsynchronisation SOLLTE sowohl für die Systemmanagement-Lösung als auch für die zu verwaltenden Systeme über alle Standorte der Institution sichergestellt werden. Dafür SOLLTE eine gemeinsame Referenzzeit benutzt werden.

**OPS.1.1.7.A24 Automatisierte Überprüfung von sicherheitsrelevanten Konfigurationen durch geeignete Detektionssysteme (H)**

Sicherheitsrelevante Konfigurationen der Systemmanagement-Lösung und der zu verwaltenden Systeme SOLLTEN durch geeignete Detektionssysteme regelmäßig auf Abweichungen vom Sollzustand sowie auf potenzielle Schwachstellen überprüft werden.

**OPS.1.1.7.A25 Protokollierung und Reglementierung von Systemmanagement-Sitzungen (H)**

Die Sitzungsinhalte, insbesondere die Aktivitäten von Benutzenden auf der Systemmanagement-Lösung sowie sämtliche direkte Zugriffe auf zu verwaltende Systeme, SOLLTEN kontinuierlich durch eine technische Lösung protokolliert und reglementiert werden. Dabei SOLLTEN die Aktivitäten auf Befehlsebene, d. h. manuelle und automatisierte Befehle, kontrolliert und gegebenenfalls unterbunden werden.

Während der Überwachung SOLLTE nicht nur bei konkreten Regelverstößen, sondern auch bei Anomalien im Benutzendenverhalten eine Alarmierung erfolgen.

**OPS.1.1.7.A26 Entkopplung von Zugriffen auf die Systemmanagement-Lösung (H)**

Jeder administrative Zugriff auf die Systemmanagement-Lösung SOLLTE durch die Nutzung von Sprungservern abgesichert werden.

# 4. Weiterführende Informationen

## 4.1. Wissenswertes

Für den Baustein OPS.1.1.7 *Systemmanagement* sind keine weiterführenden Informationen vorhanden.

Bundesamt
für Sicherheit in der
Informationstechnik

# OPS.1.2.2 Archivierung

## 1. Beschreibung

### 1.1. Einleitung

Die Archivierung spielt im Dokumentenmanagementprozess eine besondere Rolle. Denn es wird einerseits erwartet, dass die digitalen Dokumente bis zum Ablauf einer vorgegebenen Aufbewahrungsfrist verfügbar sind. Andererseits soll ihre Vertraulichkeit und Integrität bewahrt bleiben. Zusätzlich muss der Kontext erhalten werden, damit der jeweilige gespeicherte Vorgang rekonstruierbar ist.

Während der gesamten Dauer der Langzeitspeicherung müssen daher entsprechende Maßnahmen zur Informationserhaltung und, falls erforderlich, Maßnahmen zur Beweiswerterhaltung umgesetzt werden.

Im deutschen informationstechnischen Sprachgebrauch wird mitunter der Begriff „elektronische Archivierung" synonym zum Begriff „elektronische Langzeitspeicherung" verwendet. Zur besseren Verständlichkeit wird in diesem Baustein daher allgemein nur von „Archivierung" oder auch „digitalem Langzeitarchiv" gesprochen. Ein IT-Verfahren zur Aufbewahrung elektronischer Dokumente wird als „Archivsystem" bzw. „digitales Archiv" oder „Langzeitspeicher" bezeichnet. Die Aufbewahrungsdauer der Dokumente bemisst sich nach den rechtlichen und sonstigen Vorgaben sowie dem Anwendungszweck der Daten.

Der in diesem Baustein verwendete Begriff „Dokumente" beinhaltet Daten und digitale Dokumente, sofern sie nicht ausdrücklich in anderer Bedeutung gebraucht werden.

Aus rechtlicher Sicht ist der Begriff „Archivierung" in Deutschland durch die Archivgesetze des Bundes und der Länder konkretisiert und belegt. „Archivierung" im juristisch korrekten Sinne betrifft allein Unterlagen der öffentlichen Verwaltung. Sie bezieht sich darauf, dass Unterlagen einer Behörde, sobald sie für deren Zwecke nicht mehr benötigt werden, ausgesondert und durch eine zuständige staatliche Einrichtung (Bundesarchiv) auf unbegrenzte Zeit verwahrt werden sollen (vergleiche §§ 1 und 2 BarchG). Diese Art der Archivierung ist von der in diesem Baustein betrachteten zeitlich beschränkten Aufbewahrung zu unterscheiden.

### 1.2. Zielsetzung

Der Baustein beschreibt, wie digitale Dokumente langfristig, sicher, unveränderbar und wieder reproduzierbar archiviert werden können. Dazu werden Anforderungen definiert, mit denen sich ein Archivsystem sicher planen, umsetzen und betreiben lässt.

Die Aufbewahrung von Papierdokumenten wird in diesem Baustein nicht betrachtet, es werden aber Anforderungen gestellt, wie diese digitalisiert und archiviert werden können.

### 1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.2.2 *Archivierung* ist auf den Informationsverbund einmal anzuwenden, wenn eine Langzeitarchivierung von elektronischen Dokumenten erfolgt. Dabei kann eine Langzeitarchivierung aufgrund von externen oder internen Vorgaben erforderlich sein oder es ist bereits ein System zur Langzeitarchivierung elektronischer Dokumente im Betrieb.

Der Baustein behandelt nicht die zeitlich unbegrenzte Archivierung im Sinne der Archivgesetze des Bundes und der Länder.

Der vorliegende Baustein beschreibt Sicherheitsmaßnahmen, mit denen elektronische Dokumente für die Langzeitspeicherung im Rahmen von geltenden Aufbewahrungsfristen aufbewahrt und erhalten werden können. Maßnahmen für eine operative Datensicherung werden in diesem Baustein nicht behandelt. Anforderungen dazu werden in CON.3 *Datensicherungskonzept* dargestellt.

Ein digitaler Langzeitspeicher besteht aus einzelnen Komponenten, z. B. einer Datenbank. Wie sich solche Komponenten detailliert sicher betreiben lassen, ist jedoch ebenfalls nicht Thema des vorliegenden Bausteins. Dazu sind zusätzlich die Anforderungen aus den entsprechenden Bausteinen, wie APP.4.3 *Relationale Datenbanken*, SYS.1.1 *Allgemeiner Server* sowie SYS.1.8 *Speicherlösungen*, zu berücksichtigen.

# 2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.2.2 *Archivierung* von besonderer Bedeutung.

## 2.1. Überalterung von Archivsystemen

Archivierte Daten sollen typischerweise über einen sehr langen Zeitraum gespeichert bleiben. Während dieses Zeitraums können die zugrundeliegenden technischen Systemkomponenten, Speichermedien und Datenformate aber physisch oder technisch altern und dadurch unbrauchbar werden. Es können sich z. B. im Laufe der Zeit Probleme mit der Kompatibilität der verwendeten Datenformate ergeben.

Wird auf den Alterungsprozess nicht reagiert, ist langfristig damit zu rechnen, dass beispielsweise archivierte Rohdaten nicht mehr von den Archivmedien lesbar sind. Auch können archivierte Daten durch physische Fehler an Archivsystem und -medien verändert werden.

## 2.2. Unzureichende Ordnungskriterien für Archive

Elektronische Archive können sehr große Datenmengen enthalten. Die einzelnen Datensätze werden dabei nach bestimmten Ordnungskriterien abgelegt, die nach Indexdaten der Geschäftsanwendungen und Indexdaten des Archivsystems unterschieden werden. Werden ungeeignete Ordnungskriterien verwendet, können archivierte Dokumente eventuell nicht mehr oder nur sehr aufwändig recherchiert werden. Auch ist es möglich, dass die Semantik der Dokumente nicht eindeutig bestimmbar ist. Durch eine ungeeignete oder begrenzte Auswahl von Ordnungskriterien könnten auch die Ziele der Aufbewahrung verfehlt werden, z. B. die Nachweisfähigkeit gegenüber Dritten.

## 2.3. Unbefugte Archivzugriffe aufgrund unzureichender Protokollierung

Unbefugte Archivzugriffe werden üblicherweise mithilfe von Protokolldateien aufgedeckt. Wurde jedoch nicht umfangreich genug protokolliert, könnten solche Zugriffe nicht entdeckt werden. In der Folge könnten Angreifende unbemerkt an die dort gespeicherten Informationen gelangen und sie z. B. kopieren oder verändern.

## 2.4. Unzulängliche Übertragung von Papierdaten in ein elektronisches Archiv

Wenn Dokumente eingescannt werden, kann dabei das Erscheinungsbild oder die Semantik der aufgenommenen Daten verfälscht werden. Auch können dabei Dokumente verloren gehen. Dadurch können die Informationen im Dokument falsch interpretiert und berechnet werden, z. B. wenn wichtige Teile des Dokuments oder des Dokumentenstapels beim Scannen vergessen werden.

## 2.5. Unzureichende Erneuerung von kryptografischen Verfahren bei der Archivierung

Kryptografische Verfahren, die z. B. bei Signaturen, Siegeln, Zeitstempeln, technischen Beweisdaten (Evidence Records) oder Verschlüsselungen verwendet werden, müssen regelmäßig an den aktuellen Stand der Technik angepasst werden, damit die Schutzwirkung erhalten bleibt. Geschieht dies nicht, kann beispielsweise aufgrund einer veralteten unsicheren Signatur die Integrität des Dokumentes nicht mehr garantiert werden. Darüber hinaus wird die Datei eventuell nicht als Beweismittel vor Gericht zugelassen, selbst wenn das Dokument noch völlig korrekt ist. Auch geht so die Vertraulichkeit eines verschlüsselten Dokumentes verloren.

## 2.6. Unzureichende Revisionen der Archivierung

Wenn der Archivierungsprozess zu selten oder zu ungenau überprüft wird, kann dies dazu führen, dass die Fehlfunktionen nicht erkannt werden. Damit kann die Integrität der archivierten Dokumente selbst angezweifelt werden. Hieraus können sich für die Institution rechtliche und wirtschaftliche Nachteile ergeben: So kann unter Um-

ständen eine Datei nicht als Beweismittel vor Gericht zugelassen werden, weil nicht ausgeschlossen werden kann, dass sie manipuliert wurde.

### 2.7. Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Archivierung

Bei der Archivierung von elektronischen Dokumenten sind verschiedene rechtliche Rahmenbedingungen zu beachten. Werden diese nicht eingehalten, kann das zivil- oder strafrechtliche Konsequenzen haben, z. B. bei Mindestaufbewahrungsfristen, die sich aus steuerlichen, haushaltsrechtlichen oder sonstigen Gründen ergeben.

## 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.2.2 *Archivierung* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

| Zuständigkeiten | Rollen |
|---|---|
| Grundsätzlich zuständig | Fachverantwortliche |
| Weitere Zuständigkeiten | Benutzende, IT-Betrieb, Institutionsleitung |

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

### 3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

#### OPS.1.2.2.A1 Ermittlung von Einflussfaktoren für die elektronische Archivierung (B)

Bevor entschieden wird, welche Verfahren und Produkte für die elektronische Archivierung eingesetzt werden, MÜSSEN die technischen, rechtlichen und organisatorischen Einflussfaktoren ermittelt und dokumentiert werden. Die Ergebnisse MÜSSEN in das Archivierungskonzept einfließen.

#### OPS.1.2.2.A2 Entwicklung eines Archivierungskonzepts (B)

Es MUSS definiert werden, welche Ziele mit der Archivierung erreicht werden sollen. Hierbei MUSS insbesondere berücksichtigt werden, welche Regularien einzuhalten sind, welche Mitarbeitende zuständig sind und welcher Funktions- und Leistungsumfang angestrebt wird.

Die Ergebnisse MÜSSEN in einem Archivierungskonzept erfasst werden. Die Institutionsleitung MUSS in diesen Prozess einbezogen werden. Das Archivierungskonzept MUSS regelmäßig an die aktuellen Gegebenheiten der Institution angepasst werden.

#### OPS.1.2.2.A3 Geeignete Aufstellung von Archivsystemen und Lagerung von Archivmedien (B) [IT-Betrieb]

Die IT-Komponenten eines Archivsystems MÜSSEN in gesicherten Räumen aufgestellt werden. Es MUSS sichergestellt sein, dass nur berechtigte Personen die Räume betreten dürfen. Archivspeichermedien MÜSSEN geeignet gelagert werden.

#### OPS.1.2.2.A4 Konsistente Indizierung von Daten bei der Archivierung (B) [IT-Betrieb, Benutzende]

Alle in einem Archiv abgelegten Daten, Dokumente und Datensätze MÜSSEN eindeutig indiziert werden. Dazu MUSS bereits während der Konzeption festgelegt werden, welche Struktur und welchen Umfang die Indexangaben für ein Archiv haben sollen.

#### OPS.1.2.2.A5 Regelmäßige Aufbereitung von archivierten Datenbeständen (B) [IT-Betrieb]

Über den gesamten Archivierungszeitraum hinweg MUSS sichergestellt werden, dass

- das verwendete Datenformat von den benutzten Anwendungen verarbeitet werden kann,
- die gespeicherten Daten auch zukünftig lesbar und so reproduzierbar sind, dass Semantik und Beweiskraft beibehalten werden,
- das benutzte Dateisystem auf dem Speichermedium von allen beteiligten Komponenten verarbeitet werden kann,
- die Speichermedien jederzeit technisch einwandfrei gelesen werden können sowie
- die verwendeten kryptografischen Verfahren zur Verschlüsselung und zum Beweiswerterhalt mittels digitaler Signatur, Siegel, Zeitstempel oder technischen Beweisdaten (Evidence Records) dem Stand der Technik entsprechen.

#### OPS.1.2.2.A6 Schutz der Integrität der Indexdatenbank von Archivsystemen (B) [IT-Betrieb]

Die Integrität der Indexdatenbank MUSS sichergestellt und überprüfbar sein. Außerdem MUSS die Indexdatenbank regelmäßig gesichert werden. Die Datensicherungen MÜSSEN wiederherstellbar sein. Mittlere und große Archive SOLLTEN über redundante Indexdatenbanken verfügen.

#### OPS.1.2.2.A7 Regelmäßige Datensicherung der System- und Archivdaten (B) [IT-Betrieb]

Alle Archivdaten, die zugehörigen Indexdatenbanken sowie die Systemdaten MÜSSEN regelmäßig gesichert werden (siehe CON.3 *Datensicherungskonzept*).

#### OPS.1.2.2.A8 Protokollierung der Archivzugriffe (B) [IT-Betrieb]

Alle Zugriffe auf elektronische Archive MÜSSEN protokolliert werden. Dafür SOLLTEN Datum, Uhrzeit, Benutzender, Client und die ausgeführten Aktionen sowie Fehlermeldungen aufgezeichnet werden. Im Archivierungskonzept SOLLTE festgelegt werden, wie lange die Protokolldaten aufbewahrt werden.

Die Protokolldaten der Archivzugriffe SOLLTEN regelmäßig ausgewertet werden. Dabei SOLLTEN die institutionsinternen Vorgaben beachtet werden.

Auch SOLLTE definiert sein, welche Ereignisse welchen Mitarbeitenden angezeigt werden, wie z. B. Systemfehler, Timeouts oder wenn Datensätze kopiert werden. Kritische Ereignisse SOLLTEN sofort nach der Erkennung geprüft und, falls nötig, weiter eskaliert werden.

#### OPS.1.2.2.A9 Auswahl geeigneter Datenformate für die Archivierung von Dokumenten (B) [IT-Betrieb]

Für die Archivierung MUSS ein geeignetes Datenformat ausgewählt werden. Es MUSS gewährleisten, dass sich Archivdaten sowie ausgewählte Merkmale des ursprünglichen Dokumentmediums langfristig und originalgetreu reproduzieren lassen.

Die Dokumentstruktur des ausgewählten Datenformats MUSS eindeutig interpretierbar und elektronisch verarbeitbar sein. Die Syntax und Semantik der verwendeten Datenformate SOLLTE dokumentiert und von einer Standardisierungsorganisation veröffentlicht sein. Es SOLLTE für eine beweis- und revisionssichere Archivierung ein verlustfreies Bildkompressionsverfahren benutzt werden.

## 3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

#### OPS.1.2.2.A10 Erstellung einer Richtlinie für die Nutzung von Archivsystemen (S) [IT-Betrieb]

Es SOLLTE sichergestellt werden, dass Mitarbeitende das Archivsystem so benutzen, wie es im Archivierungskonzept vorgesehen ist. Dazu SOLLTE eine Administrations- und eine Benutzungsrichtlinie erstellt werden. Die Administrationsrichtlinie SOLLTE folgende Punkte enthalten:

- Festlegung der Verantwortung für Betrieb und Administration,
- Vereinbarungen über Leistungsparameter beim Betrieb (unter anderem Service Level Agreements),

- Modalitäten der Vergabe von Zutritts- und Zugriffsrechten,
- Modalitäten der Vergabe von Zugangsrechten zu den vom Archiv bereitgestellten Diensten,
- Regelungen zum Umgang mit archivierten Daten und Archivmedien,
- Überwachung des Archivsystems und der Umgebungsbedingungen,
- Regelungen zur Datensicherung,
- Regelungen zur Protokollierung sowie
- Trennung von Produzenten und Konsumenten (OAIS-Modell).

**OPS.1.2.2.A11 Einweisung in die Administration und Bedienung des Archivsystems (S) [IT-Betrieb, Benutzende]**

Die zuständigen Mitarbeitende des IT-Betriebs und die Benutzenden SOLLTEN für ihren Aufgabenbereich geschult werden.

Die Schulung der Mitarbeitenden des IT-Betriebs SOLLTE folgende Themen umfassen:

- Systemarchitektur und Sicherheitsmechanismen des verwendeten Archivsystems und des darunterliegenden Betriebssystems,
- Installation und Bedienung des Archivsystems und Umgang mit Archivmedien,
- Dokumentation der Administrationstätigkeiten sowie
- Eskalationsprozeduren.

Die Schulung der Benutzende SOLLTE folgende Themen umfassen:

- Umgang mit dem Archivsystem,
- Bedienung des Archivsystems sowie
- rechtliche Rahmenbedingungen der Archivierung.

Die Durchführung der Schulungen sowie die Teilnahme SOLLTEN dokumentiert werden.

**OPS.1.2.2.A12 Überwachung der Speicherressourcen von Archivmedien (S) [IT-Betrieb]**

Die auf den Archivmedien vorhandene freie Speicherkapazität SOLLTE kontinuierlich überwacht werden. Sobald ein definierter Grenzwert unterschritten wird, MÜSSEN zuständige Mitarbeitende automatisch alarmiert werden. Die Alarmierung SOLLTE rollenbezogen erfolgen. Es MÜSSEN immer ausreichend leere Archivmedien verfügbar sein, um Speicherengpässen schnell vorbeugen zu können.

**OPS.1.2.2.A13 Regelmäßige Revision der Archivierungsprozesse (S)**

Es SOLLTE regelmäßig überprüft werden, ob die Archivierungsprozesse noch korrekt und ordnungsgemäß funktionieren. Dazu SOLLTE eine Checkliste erstellt werden, die Fragen zu Verantwortlichkeiten, Organisationsprozessen, zum Einsatz der Archivierung, zur Redundanz der Archivdaten, zur Administration und zur technischen Beurteilung des Archivsystems enthält. Die Auditergebnisse SOLLTEN nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen werden. Abweichungen SOLLTE nachgegangen werden.

**OPS.1.2.2.A14 Regelmäßige Beobachtung des Marktes für Archivsysteme (S) [IT-Betrieb]**

Der Markt für Archivsysteme SOLLTE regelmäßig und systematisch beobachtet werden. Dabei SOLLTEN unter anderem folgende Kriterien beobachtet werden:

- Veränderungen bei Standards,
- Wechsel der Technik bei herstellenden Unternehmen von Hard- und Software,
- veröffentlichte Sicherheitslücken oder Schwachstellen sowie
- der Verlust der Sicherheitseignung bei kryptografischen Algorithmen.

#### OPS.1.2.2.A15 Regelmäßige Aufbereitung von kryptografisch gesicherten Daten bei der Archivierung (S) [IT-Betrieb]

Es SOLLTE kontinuierlich beobachtet werden, wie sich das Gebiet der Kryptografie entwickelt, um beurteilen zu können, ob ein Algorithmus weiterhin zuverlässig und ausreichend sicher ist (siehe auch OPS.1.2.2.A20 *Geeigneter Einsatz kryptografischer Verfahren bei der Archivierung*).

Archivdaten, die mit kryptografischen Verfahren gesichert wurden, die sich in absehbarer Zeit nicht mehr zur Sicherung eignen werden, SOLLTEN rechtzeitig mit geeigneten Verfahren neu gesichert werden.

#### OPS.1.2.2.A16 Regelmäßige Erneuerung technischer Archivsystem-Komponenten (S) [IT-Betrieb]

Archivsysteme SOLLTEN über lange Zeiträume auf dem aktuellen technischen Stand gehalten werden. Neue Hard- und Software SOLLTE vor der Installation in einem laufenden Archivsystem ausführlich getestet werden. Wenn neue Komponenten in Betrieb genommen oder neue Dateiformate eingeführt werden, SOLLTE ein Migrationskonzept erstellt werden. Darin SOLLTEN alle Änderungen, Tests und erwarteten Testergebnisse beschrieben sein. Die Konvertierung der einzelnen Daten SOLLTE dokumentiert werden (Transfervermerk).

Wenn Archivdaten in neue Formate konvertiert werden, SOLLTE geprüft werden, ob die Daten aufgrund rechtlicher Anforderungen zusätzlich in ihren ursprünglichen Formaten zu archivieren sind.

#### OPS.1.2.2.A17 Auswahl eines geeigneten Archivsystems (S) [IT-Betrieb]

Ein neues Archivsystem SOLLTE immer auf Basis der im Archivierungskonzept beschriebenen Vorgaben ausgewählt werden. Es SOLLTE die dort formulierten Anforderungen erfüllen.

#### OPS.1.2.2.A18 Verwendung geeigneter Archivmedien (S) [IT-Betrieb]

Für die Archivierung SOLLTEN geeignete Medien ausgewählt und benutzt werden. Dabei SOLLTEN folgende Aspekte berücksichtigt werden:

- das zu archivierende Datenvolumen,
- die mittleren Zugriffszeiten sowie
- die mittleren gleichzeitigen Zugriffe auf das Archivsystem.

Ebenfalls SOLLTEN die Archivmedien die Anforderungen an eine Langzeitarchivierung hinsichtlich Revisionssicherheit und Lebensdauer erfüllen.

#### OPS.1.2.2.A19 Regelmäßige Funktions- und Recoverytests bei der Archivierung (S) [IT-Betrieb]

Für die Archivierung SOLLTEN regelmäßige Funktions- und Recoverytests durchgeführt werden. Die Archivierungsdatenträger SOLLTEN mindestens einmal jährlich daraufhin überprüft werden, ob sie noch lesbar und integer sind. Für die Fehlerbehebung SOLLTEN geeignete Prozesse definiert werden.

Weiterhin SOLLTEN die Hardwarekomponenten des Archivsystems regelmäßig auf ihre einwandfreie Funktion hin geprüft werden. Es SOLLTE regelmäßig geprüft werden, ob alle Archivierungsprozesse fehlerfrei funktionieren.

## 3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

#### OPS.1.2.2.A20 Geeigneter Einsatz kryptografischer Verfahren bei der Archivierung (H) [IT-Betrieb]

Um lange Aufbewahrungsfristen abdecken zu können, SOLLTEN Archivdaten nur mit kryptografischen Verfahren auf Basis aktueller Standards und Normen gesichert werden.

#### OPS.1.2.2.A21 Übertragung von Papierdaten in elektronische Archive (H)

Werden z. B. Dokumente auf Papier digitalisiert und in ein elektronisches Archiv überführt, SOLLTE sichergestellt werden, dass die digitale Kopie mit dem Originaldokument bildlich und inhaltlich übereinstimmt.

# 4. Weiterführende Informationen

## 4.1. Wissenswertes

Die Bundesnetzagentur (BNetzA) listet in ihrer Veröffentlichung „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung: Auflistung geeigneter Algorithmen und Parameter" als geeignet eingestufte Algorithmen und Parameter auf.

Das Deutsche Institut für Normung e. V. (DIN) definiert in der DIN 31644:2012-04 „Information und Dokumentation – Kriterien für vertrauenswürdige digitale Langzeitarchive" Kriterien für vertrauenswürdige digitale Langzeitarchive. In der DIN 31647:2015-05 „Information und Dokumentation – Beweiswerterhaltung kryptographisch signierter Dokumente" werden technische und sicherheitsrelevante Anforderungen an die langfristige Aufbewahrung von digital signierten Dokumenten unter Wahrung der Rechtskraft der digitalen Signatur definiert.

Das BSI hat in seiner technischen Richtlinie „BSI TR-03138 RESISCAN: Ersetzendes Scannen" die sicherheitsrelevanten technischen und organisatorischen Maßnahmen, die beim ersetzenden Scannen zu berücksichtigen sind, zusammengestellt.

In der technischen Richtlinie „BSI TR-03125 TR-ESOR: Beweiswerterhaltung kryptographisch signierter Dokumente" nebst seinen Anhängen stellt das BSI einen Leitfaden zur Verfügung, der beschreibt, wie elektronisch signierte Daten und Dokumente über lange Zeiträume, bis zum Ende der Aufbewahrungsfristen, im Sinne eines rechtswirksamen Beweiswerterhalts vertrauenswürdig gespeichert werden können.

Bundesamt
für Sicherheit in der
Informationstechnik

# OPS.1.2.4 Telearbeit

## 1. Beschreibung

### 1.1. Einleitung

Unter Telearbeit wird jede auf die Informations- und Kommunikationstechnik gestützte Tätigkeit verstanden, die ganz oder teilweise außerhalb der Geschäftsräume und Gebäude der Institution verrichtet wird. Bei der heimbasierten Telearbeit arbeiten die Mitarbeitenden regelmäßig tages- oder stundenweise abwechselnd an ihrem Arbeitsplatz in den Räumlichkeiten der Institution und am häuslichen Arbeitsplatz.

### 1.2. Zielsetzung

Das Ziel des Bausteins ist der Schutz von Informationen, die während der Telearbeit gespeichert, verarbeitet und übertragen werden. Dazu werden typische Gefährdungen aufgezeigt und spezielle Anforderungen an die sichere Telearbeit definiert.

### 1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.2.4 *Telearbeit* ist für jeden Telearbeitsplatz anzuwenden.

Dieser Baustein konzentriert sich auf die Form der Telearbeit, die im häuslichen Umfeld durchgeführt wird (heimbasierte Telearbeit). Es wird davon ausgegangen, dass zwischen dem Telearbeitsplatz und der Institution eine sichere Telekommunikationsverbindung besteht, die es ermöglicht, geeignet Informationen auszutauschen und auf Daten auf dem Server der Institution zuzugreifen. Die Anforderungen dieses Bausteins umfassen die folgenden drei Bereiche:

- die Organisation der Telearbeit,
- den Arbeitsplatz-PCs der Mitarbeitenden und
- die Kommunikationsverbindung zwischen Telearbeitsrechnern und Institution.

Sicherheitsanforderungen an die Infrastruktur des Telearbeitsplatzes werden im vorliegenden Baustein nicht berücksichtigt, sondern sind im Baustein INF.8 *Häuslicher Arbeitsplatz* beschrieben. Anforderungen an einen nicht dauerhaft eingerichteten Arbeitsplatz sind im Baustein INF.9 *Mobiler Arbeitsplatz* zu finden.

Detaillierte Empfehlungen, wie die IT-Systeme konfiguriert und abgesichert werden können, werden nicht im Rahmen dieses Bausteins behandelt. Sie sind in SYS.2.1 *Allgemeiner Client* sowie in den betriebssystemspezifischen System-Bausteinen zu finden. Weitere für die Telearbeit relevante Sicherheitsaspekte, wie z. B. für WLAN, werden in den Bausteinen der Teilschichten NET.2 *Funknetze* oder NET.4 *Telekommunikation* betrachtet.

Sofern Daten, die bei der Telearbeit verändert wurden, nicht unmittelbar auf IT-Systemen der Institution gespeichert werden, muss geregelt werden, wie eine Datensicherung durchgeführt wird. Anforderungen dazu sind im Baustein CON.3 *Datensicherungskonzept* zu finden.

## 2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.2.4 *Telearbeit* von besonderer Bedeutung.

### 2.1. Fehlende oder unzureichende Regelungen für den Telearbeitsplatz

Die Nutzung eines Telearbeitsplatzes erfordert ergänzende organisatorische Absprachen zwischen den Mitarbeitenden und den Führungskräften. Zudem brauchen sie Handlungsanweisungen für den Fall, dass sicherheitsrelevante Vorkommnisse am Telearbeitsplatz eintreten. Gelangen beispielsweise vertrauliche Informationen in die Hände Dritter, können schwerwiegende Schäden für die Institution entstehen.

### 2.2. Unerlaubte private Nutzung des dienstlichen Telearbeitsrechners

Im häuslichen Bereich kann leichter nicht geprüfte und nicht freigegebene Hard- oder Software eingesetzt werden und so durch unbedachtes Handeln beispielsweise Schadsoftware auf den Telearbeitsrechner gelangen. Dadurch könnten vertrauliche Informationen kompromittiert werden.

### 2.3. Verzögerungen durch temporär eingeschränkte Erreichbarkeit der Mitarbeitenden

Haben die Mitarbeitenden keine festen Arbeitszeiten am Telearbeitsplatz und werden keine festen Zeiten vereinbart, an denen sie erreichbar sein müssen, kann aufgrund dessen der Arbeitsablauf verzögert werden.

### 2.4. Mangelhafte Einbindung der Mitarbeitenden in den Informationsfluss

Da die Mitarbeitenden nicht täglich in der Institution sind, haben sie weniger Gelegenheit, am direkten Informationsaustausch mit den Führungskräften sowie den Kollegen und Kolleginnen teilzuhaben. Es ist daher möglich, dass Telearbeitende insbesondere mündlich weitergegebene Informationen nicht oder erst verzögert erhalten. Hierdurch können Arbeitsabläufe und betriebliche Prozesse gestört und die Produktivität des oder der Mitarbeitenden eingeschränkt werden.

### 2.5. Nichtbeachtung von Sicherheitsmaßnahmen

Am Telearbeitsplatz können beispielsweise fehlende Kontrollmöglichkeiten dazu führen, dass Mitarbeitende empfohlene oder angeordnete Sicherheitsmaßnahmen nicht oder nicht in vollem Umfang umsetzen. So können z. B. vertrauliche Informationen in die Hände Dritter geraten.

## 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.2.4 *Telearbeit* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

| Zuständigkeiten | Rollen |
|---|---|
| Grundsätzlich zuständig | Informationssicherheitsbeauftragte (ISB) |
| Weitere Zuständigkeiten | Mitarbeitende, IT-Betrieb, Vorgesetzte, Personalabteilung |

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

### 3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

#### OPS.1.2.4.A1 Regelungen für Telearbeit (B) [Vorgesetzte, Personalabteilung]

Alle relevanten Aspekte der Telearbeit MÜSSEN geregelt werden. Zu Informationszwecken MÜSSEN den Telearbeitenden die geltenden Regelungen oder ein dafür vorgesehenes Merkblatt ausgehändigt werden, das die zu beach-

tenden Sicherheitsmaßnahmen erläutert. Alle strittigen Punkte MÜSSEN entweder durch Betriebsvereinbarungen oder durch zusätzlich zum Arbeitsvertrag getroffene individuelle Vereinbarungen zwischen dem Mitarbeitenden und der Institution geregelt werden. Die Regelungen MÜSSEN regelmäßig aktualisiert werden.

#### OPS.1.2.4.A2 Sicherheitstechnische Anforderungen an den Telearbeitsrechner (B)

Es MÜSSEN sicherheitstechnische Anforderungen festgelegt werden, die ein IT-System für die Telearbeit erfüllen muss.

Es MUSS sichergestellt werden, dass nur autorisierte Personen Zugang zu den Telearbeitsrechnern haben. Darüber hinaus MUSS der Telearbeitsrechner so abgesichert werden, dass er nur für autorisierte Zwecke benutzt werden kann.

#### OPS.1.2.4.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

#### OPS.1.2.4.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

#### OPS.1.2.4.A5 Sensibilisierung und Schulung der Mitarbeitenden (B)

Anhand eines Leitfadens MÜSSEN die Mitarbeitenden für die Gefahren sensibilisiert werden, die mit der Telearbeit verbunden sind. Außerdem MÜSSEN sie in die entsprechenden Sicherheitsmaßnahmen der Institution eingewiesen und im Umgang mit diesen geschult werden. Die Schulungs- und Sensibilisierungsmaßnahmen für Mitarbeitenden SOLLTEN regelmäßig wiederholt werden.

## 3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

#### OPS.1.2.4.A6 Erstellen eines Sicherheitskonzeptes für Telearbeit (S)

Es SOLLTE ein Sicherheitskonzept für die Telearbeit erstellt werden, das Sicherheitsziele, Schutzbedarf, Sicherheitsanforderungen sowie Risiken beschreibt. Das Konzept SOLLTE regelmäßig aktualisiert und überarbeitet werden. Das Sicherheitskonzept zur Telearbeit SOLLTE auf das übergreifende Sicherheitskonzept der Institution abgestimmt werden.

#### OPS.1.2.4.A7 Regelung der Nutzung von Kommunikationsmöglichkeiten bei Telearbeit (S) [IT-Betrieb, Mitarbeitende]

Es SOLLTE klar geregelt werden, welche Kommunikationsmöglichkeiten bei der Telearbeit unter welchen Rahmenbedingungen genutzt werden dürfen. Die dienstliche und private Nutzung von Internetdiensten bei der Telearbeit SOLLTE geregelt werden. Dabei SOLLTE auch geklärt werden, ob eine private Nutzung generell erlaubt oder unterbunden wird.

#### OPS.1.2.4.A8 Informationsfluss zwischen Mitarbeitenden und Institution (S) [Vorgesetzte, Mitarbeitende]

Ein regelmäßiger innerbetrieblicher Informationsaustausch zwischen den Mitarbeitenden und der Institution SOLLTE gewährleistet sein. Alle Mitarbeitenden SOLLTEN zeitnah über geänderte Sicherheitsanforderungen und andere sicherheitsrelevante Aspekte informiert werden. Allen Kollegen und Kolleginnen der jeweiligen Mitarbeitenden SOLLTE bekannt sein, wann und wo diese erreicht werden können. Technische und organisatorische Telearbeitsregelungen zur Aufgabenbewältigung, zu Sicherheitsvorfällen und sonstigen Problemen SOLLTEN geregelt und an die Mitarbeitenden kommuniziert werden.

#### OPS.1.2.4.A9 Betreuungs- und Wartungskonzept für Telearbeitsplätze (S) [IT-Betrieb, Mitarbeitende]

Für Telearbeitsplätze SOLLTE ein spezielles Betreuungs- und Wartungskonzept erstellt werden. Darin SOLLTEN folgende Aspekte geregelt werden: Kontaktperson des IT-Betriebs, Wartungstermine, Fernwartung, Transport der IT-Geräte und Einführung von Standard-Telearbeitsrechnern. Damit die Mitarbeitenden einsatzfähig bleiben, SOLLTEN für sie Kontaktpersonen für Hard- und Softwareprobleme benannt werden.

**OPS.1.2.4.A10 Durchführung einer Anforderungsanalyse für den Telearbeitsplatz (S) [IT-Betrieb]**

Bevor ein Telearbeitsplatz eingerichtet wird, SOLLTE eine Anforderungsanalyse durchgeführt werden. Daraus SOLLTE z. B. hervorgehen, welche Hard- und Software-Komponenten für den Telearbeitsplatz benötigt werden. Die Anforderungen an den jeweiligen Telearbeitsplatz SOLLTEN mit den IT-Verantwortlichen abgestimmt werden. Es SOLLTE immer festgestellt und dokumentiert werden, welchen Schutzbedarf die am Telearbeitsplatz verarbeiteten Informationen haben.

### 3.3. Anforderungen bei erhöhtem Schutzbedarf

Für diesen Baustein sind keine Anforderungen für einen erhöhten Schutzbedarf definiert.

## 4. Weiterführende Informationen

### 4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013, insbesondere in Annex A, A.6.2.1 „Mobile device policy" und A.11.2.6 „Security of equipment and assets off-premises", Informationen zum Umgang mit Telearbeit.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security", insbesondere in Area PA2 Mobile Computing, ebenfalls Vorgaben zur Telearbeit.

Das National Institute of Standards and Technology (NIST) hat im Rahmen seiner Special Publications die NIST Special Publication 800-46 als „Guide to Enterprise Telework, Remote Access and Bring Your Own Device (BYOD) Security" veröffentlicht.

Bundesamt
für Sicherheit in der
Informationstechnik

# OPS.1.2.5 Fernwartung

## 1. Beschreibung

### 1.1. Einleitung

Mit dem Begriff Fernwartung wird ein zeitlich begrenzter Zugriff auf IT-Systeme und die darauf laufenden Anwendungen bezeichnet, der von einem anderen IT-System aus erfolgt. Der Zugriff kann z. B. dazu dienen, Konfigurations-, Wartungs- oder Reparaturarbeiten durchzuführen.

Die Fernwartung kann auf unterschiedliche Weise geschehen. Bei der Fernwartung von Clients werden oft die Tastatur- und Maussignale von IT-Systemen von den Administrierenden an ein entferntes IT-System übertragen. Das entfernte IT-System überträgt die Bildschirmausgabe an das IT-System der Administrierenden. Die Administrierenden führen Aktionen auf dem entfernten IT-System so aus, als wenn sie selbst vor Ort wären (aktive Fernwartung). Bei der Fernwartung von Servern wird oft die Ein- und Ausgabe der Konsole übertragen.

Bei der passiven Fernwartung werden nur die Bildschirminhalte eines IT-Systems zu den Administrierenden übertragen. Administrierende erteilen den Benutzenden vor Ort Anweisungen, die von ihnen ausgeführt und von den Administrierenden beobachtet werden. Allerdings erweist sich dieses Vorgehen in der Praxis meist als sehr zeitintensiv und umständlich, weshalb häufig dem IT-Betrieb voller Zugriff über das IT-System zugewiesen wird.

Da sich viele IT-Systeme außerhalb der Reichweite ihrer Administrierenden befinden (z. B. in entfernten Rechenzentren, Industrieanlagen oder einem Außenstandort ohne IT-Personal), wird Fernwartung in vielen Institutionen eingesetzt. Bei der Fernwartung wird oft über unsichere Netze auf interne IT-Systeme und Anwendungen einer Institution zugegriffen. Wegen der dabei bestehenden tiefgreifenden Eingriffsmöglichkeiten in diese IT-Systeme und Anwendungen ist die Absicherung von Fernwartungskomponenten von besonderer Bedeutung.

### 1.2. Zielsetzung

Ziel dieses Bausteins ist der Schutz der Informationen, die bei der Fernwartung gespeichert, verarbeitet und übertragen werden sowie der Schutz der Fernwartungsschnittstellen von IT-Systemen. Zu diesem Zweck werden Anforderungen an die Fernwartung gestellt, die sich gleichermaßen auf Funktionen der aktiven und passiven Fernwartung beziehen.

### 1.3. Abgrenzung und Modellierung

Der Baustein ist auf alle Zielobjekte im Informationsverbund anzuwenden, bei denen Fernwartung genutzt wird.

Dieser Baustein betrachtet die Fernwartung überwiegend aus der Sicht des IT-Betriebs und gibt Hinweise für Administrierende, wie Fernwartung eingesetzt werden kann. Die Sicherheitsaspekte der eingesetzten Kommunikationsverbindungen und Authentisierungsmechanismen sowie die Absicherung der Fernwartungszugänge sind wichtige Bestandteile dieses Bausteins. Dennoch werden darin nicht alle relevanten Aspekte der mit einer Fernwartung in Verbindung stehenden Geschäftsprozesse abgedeckt. Vor allem die Bausteine OPS.1.1.3 *Patch- und Änderungsmanagement*, ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit*, CON.1 *Kryptokonzept* und CON.3 *Datensicherungskonzept* sind zusätzlich zu beachten. Ebenso sind die Vorgaben der Bausteinschicht NET *Netze und Kommunikation* umzusetzen, sofern diese direkt mit der Fernwartung in Verbindung stehen.

Wird die Fernwartung von externen Dienstleistenden durchgeführt, muss zudem der Baustein OPS.2.3 *Nutzung von Outsourcing* beachtet werden. Werden cloudbasierte Fernwartungsprodukte verwendet, müssen auch die allgemeinen Anforderungen aus dem Baustein OPS.2.2 *Cloud-Nutzung* erfüllt werden.

Anforderungen zur Absicherung der Fernwartung mittels Firewalls sind nicht Bestandteil dieses Bausteins. Anforderungen dazu sind im Baustein NET.3.2 *Firewall* zu finden.

Grundsätzliche Aspekte der IT-Administration werden ebenfalls nicht in diesem Baustein betrachtet. Sie sind im Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration* zu finden. Ebenfalls nicht betrachtet werden Anforderungen des Systemmanagements. Diese sind im Baustein OPS.1.1.7 *Systemmanagement* zu finden.

Nicht im Fokus des Bausteins steht die Fernwartung im industriellen Umfeld. Anforderungen dazu sind im Baustein IND.3.2 *Fernwartung im industriellen Umfeld* zu finden.

# 2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.2.5 *Fernwartung* von besonderer Bedeutung.

## 2.1. Unzureichende Kenntnisse über Regelungen der Fernwartung

Administrierende, die Fernwartung einrichten und nutzen, sind auf Regelungen angewiesen, die festlegen, wie Fernwartung verwendet werden soll. Beispielsweise ist es notwendig festzulegen, wie Anwendungen zur Fernwartung konfiguriert werden sollen. Ansonsten können mit der Fernwartung zusätzliche Risiken für das interne Netz entstehen. Werden den Beteiligten die Regelungen zur Fernwartung nicht mitgeteilt, ergeben sich Gefahren für den IT-Betrieb. Beispielsweise könnte eine Fernwartungsschnittstelle eingerichtet und dabei ein Authentisierungsverfahren mit unsicherem Passwort erlaubt werden, anstelle eines sicheren, zertifikatbasierten Verfahrens.

## 2.2. Fehlende oder unzureichende Planung und Regelung der Fernwartung

Wird die Fernwartung nicht sorgfältig geplant, aufgebaut und geregelt, kann die Sicherheit aller IT-Systeme einer Institution beeinträchtigt werden. Werden beispielsweise unsichere Kommunikationsprotokolle, Verschlüsselungsalgorithmen oder Authentisierungsmechanismen eingesetzt, können Sicherheitslücken entstehen. Über unzureichend gesicherte Fernwartungsschnittstellen kann auch ein gekoppeltes Netz eines Dritten kompromittiert werden.

## 2.3. Ungeeignete Nutzung von Authentisierung bei der Fernwartung

Bei der Fernwartung können unterschiedliche Authentisierungsmechanismen verwendet werden. Wird ein unsicheres Authentisierungsverfahren genutzt, können unberechtigte Dritte administrative Berechtigungen auf Fernwartungssystemen oder für Fernwartungswerkzeuge erlangen. Dadurch können sie auf die IT-Systeme einer Institution zugreifen und weitreichende Schäden verursachen.

Ein Beispiel hierfür ist ein Anmeldeverfahren, das nur ein kurzes Passwort verwendet. Bei einem Angriff kann dieses Passwort in kurzer Zeit erraten und sich so Zugriff auf IT-Systeme der Institution verschafft werden.

## 2.4. Fehlerhafte Fernwartung

Damit die Sicherheit und Funktionsfähigkeit von IT-Systemen und Anwendungen, auf die nur aus der Ferne zugegriffen werden kann, gewährleistet wird, ist eine professionelle und regelmäßige Fernwartung erforderlich. Werden solche IT-Systeme und Anwendungen nicht ordnungsgemäß per Fernwartung konfiguriert und gewartet, können sie im schlimmsten Fall nicht mehr genutzt werden. Laufen die Fernwartungsprozesse nicht korrekt ab, kann dies zu Fehlfunktionen einzelner Betriebssystemkomponenten führen. Außerdem können durch verspätete oder fehlerhafte IT-Systemwartungen Sicherheitslücken entstehen.

## 2.5. Verwendung unsicherer Protokolle in der Fernwartung

Die Kommunikation über öffentliche und interne Netze mittels unsicherer Protokolle stellt eine potenzielle Gefahr dar. Werden z. B. veraltete Versionen von IPSec, SSH oder SSL/TLS eingesetzt, um einen Tunnel zwischen zwei Netzen oder Endpunkten herzustellen, kann nicht gewährleistet werden, dass dieser Tunnel ausreichend sicher ist und die darin übertragenen Informationen angemessen geschützt sind. Bei einem Angriff können Schwachstellen dieser Protokolle ausgenutzt werden, um in geschützte Verbindungen eigene Inhalte einzuschleusen. Generell als unsicher gelten Protokolle, bei denen Informationen im Klartext übertragen werden.

### 2.6. Fehlende Regelungen zur Fremdnutzung der Fernwartungszugänge

Werden IT-Systeme von Dritten ferngewartet, ohne dass es dafür eine vertragliche Grundlage gibt, sind die Zuständigkeiten für die Fernwartung möglicherweise nicht klar geregelt. Dadurch können z. B. Rollentrennungen umgangen werden oder offene Fernwartungszugänge werden nicht dokumentiert.

### 2.7. Nutzung von Online-Diensten für die Fernwartung

Neben einer Fernwartung, bei der eine direkte Datenverbindung zu der betreffenden Institution aufgebaut wird, können auch Online-Dienste genutzt werden. Hierbei verbinden sich die zu administrierenden IT-Systeme mit den Servern von Online-Diensten und die Administrierenden können z. B. über einen Webbrowser auf die zu administrierenden IT-Systeme zugreifen.

Falls die Kommunikation nicht Ende-zu-Ende verschlüsselt wird, könnten die Online-Dienste den Datenaustausch mitlesen. Zusätzlich könnten auch die IT-Systeme durch unberechtigte Personen administriert werden, indem die Datenverbindung verändert wird. Bauen die IT-Systeme automatisch beim Systemstart eine Datenverbindung zum Online-Dienst auf, könnte direkt auf das IT-System zugegriffen werden, ohne dass dies den Benutzenden des IT-Systems oder den zuständigen Administrierenden bekannt ist.

### 2.8. Unbekannte Fernwartungskomponenten

Viele IT-Systeme enthalten Komponenten, die integrierte Funktionen zur Fernwartung bieten. Oft sind diese Funktionen aber schlecht dokumentiert und werden bei der Beschaffung sowie beim Betrieb von IT-Systemen nicht berücksichtigt.

Integrierte Fernwartungskomponenten haben weitreichenden Zugriff auf die IT-Systeme, in denen sie verbaut sind. Dieser Zugriff wirkt dabei oft direkt auf andere Komponenten des IT-Systems und kann so die Sicherheitsmechanismen des Betriebssystems umgehen. Zusätzlich können integrierte Fernwartungsfunktionen Schwachstellen enthalten, die einen unberechtigten Zugriff auf das IT-System vereinfachen.

## 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.2.5 *Fernwartung* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

| Zuständigkeiten | Rollen |
|---|---|
| Grundsätzlich zuständig | IT-Betrieb |
| Weitere Zuständigkeiten | Benutzende |

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

### 3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

#### OPS.1.2.5.A1 Planung des Einsatzes der Fernwartung (B)

Der Einsatz der Fernwartung MUSS an die Institution angepasst werden. Die Fernwartung MUSS hinsichtlich technischer und organisatorischer Aspekte bedarfsgerecht geplant werden. Dabei MUSS mindestens berücksichtigt werden, welche IT-Systeme ferngewartet werden sollen und wer dafür zuständig ist.

#### OPS.1.2.5.A2 Sicherer Verbindungsaufbau bei der Fernwartung von Clients (B) [Benutzende]

Wird per Fernwartung auf Desktop-Umgebungen von Clients zugegriffen, MUSS die Fernwartungssoftware so konfiguriert sein, dass sie eine Verbindung erst nach expliziter Zustimmung der Benutzenden aufbaut.

#### OPS.1.2.5.A3 Absicherung der Schnittstellen zur Fernwartung (B)

Die möglichen Zugänge und Kommunikationsverbindungen für die Fernwartung MÜSSEN auf das notwendige Maß beschränkt werden. Alle Fernwartungsverbindungen MÜSSEN nach dem Fernzugriff getrennt werden.

Es MUSS sichergestellt werden, dass Fernwartungssoftware nur auf IT-Systemen installiert ist, auf denen sie benötigt wird.

Fernwartungsverbindungen über nicht vertrauenswürdige Netze MÜSSEN verschlüsselt werden. Alle anderen Fernwartungsverbindungen SOLLTEN verschlüsselt werden.

#### OPS.1.2.5.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

## 3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

#### OPS.1.2.5.A5 Einsatz von Online-Diensten (S)

Die Institution SOLLTE festlegen, unter welchen Umständen Online-Dienste zur Fernwartung genutzt werden dürfen, bei denen die Verbindung über einen externen Server hergestellt wird. Der Einsatz solcher Dienste SOLLTE generell auf möglichst wenige Fälle beschränkt werden. Die IT-Systeme SOLLTEN keine automatisierten Verbindungen zum Online-Dienst aufbauen. Es SOLLTE sichergestellt werden, dass der eingesetzte Online-Dienst die übertragenen Informationen Ende-zu-Ende-verschlüsselt.

#### OPS.1.2.5.A6 Erstellung einer Richtlinie für die Fernwartung (S)

Die Institution SOLLTE eine Richtlinie zur Fernwartung erstellen, in der alle relevanten Regelungen zur Fernwartung dokumentiert werden. Die Richtlinie SOLLTE allen Zuständigen bekannt sein, die an der Konzeption, dem Aufbau und dem Betrieb der Fernwartung beteiligt sind.

#### OPS.1.2.5.A7 Dokumentation bei der Fernwartung (S)

Die Fernwartung SOLLTE geeignet dokumentiert werden. Aus der Dokumentation SOLLTE hervorgehen, welche Fernwartungszugänge existieren und ob diese aktiviert sind. Die Dokumente SOLLTEN an geeigneten Orten und vor unberechtigtem Zugriff geschützt abgelegt werden. Die Dokumente SOLLTEN im Rahmen des Notfallmanagements zur Verfügung stehen.

#### OPS.1.2.5.A8 Sichere Protokolle bei der Fernwartung (S)

Nur als sicher eingestufte Kommunikationsprotokolle SOLLTEN eingesetzt werden. Dafür SOLLTEN sichere kryptografische Verfahren verwendet werden. Die Stärke der verwendeten kryptografischen Verfahren und Schlüssel SOLLTE regelmäßig überprüft und bei Bedarf angepasst werden.

Wird auf die Fernwartungszugänge von IT-Systemen im internen Netz über ein öffentliches Datennetz zugegriffen, SOLLTE ein abgesichertes Virtuelles Privates Netz (VPN) genutzt werden.

#### OPS.1.2.5.A9 Auswahl und Beschaffung geeigneter Fernwartungswerkzeuge (S)

Die Auswahl geeigneter Fernwartungswerkzeuge SOLLTE sich aus den betrieblichen, sicherheitstechnischen und datenschutzrechtlichen Anforderungen der Institution ergeben. Alle Beschaffungsentscheidungen SOLLTEN mit den System- und Anwendungsverantwortlichen sowie dem oder der Informationssicherheitsbeauftragten abgestimmt werden.

**OPS.1.2.5.A10 Umgang mit Fernwartungswerkzeugen (S)**

Es SOLLTEN organisatorische Verwaltungsprozesse zum Umgang mit den ausgewählten Fernwartungswerkzeugen etabliert werden. Es SOLLTE eine Bedienungsanleitung für den Umgang mit den Fernwartungswerkzeugen vorliegen. Ergänzend zu den allgemeinen Schulungsmaßnahmen SOLLTEN Musterabläufe für die passive und die aktive Fernwartung erstellt und kommuniziert werden. Zusätzlich zu den allgemeinen Schulungsmaßnahmen SOLLTE der IT-Betrieb besonders im Umgang mit den Fernwartungswerkzeugen sensibilisiert und geschult werden. Es SOLLTE ein Ansprechpartner oder eine Ansprechpartnerin für alle fachlichen Fragen zu den Fernwartungswerkzeugen benannt werden.

**OPS.1.2.5.A11 ENTFALLEN (S)**

Diese Anforderung ist entfallen.

**OPS.1.2.5.A12 ENTFALLEN (S)**

Diese Anforderung ist entfallen.

**OPS.1.2.5.A13 ENTFALLEN (S)**

Diese Anforderung ist entfallen.

**OPS.1.2.5.A15 ENTFALLEN (S)**

Diese Anforderung ist entfallen.

**OPS.1.2.5.A16 ENTFALLEN (S)**

Diese Anforderung ist entfallen.

**OPS.1.2.5.A17 Authentisierungsmechanismen bei der Fernwartung (S)**

Für die Fernwartung SOLLTEN Mehr-Faktor-Verfahren zur Authentisierung eingesetzt werden. Die Auswahl der Authentisierungsmethode und die Gründe, die zu der Auswahl geführt haben, SOLLTEN dokumentiert werden. Fernwartungszugänge SOLLTEN im Identitäts- und Berechtigungsmanagement der Institution berücksichtigt werden.

**OPS.1.2.5.A18 ENTFALLEN (S)**

Diese Anforderung ist entfallen.

**OPS.1.2.5.A19 Fernwartung durch Dritte (S)**

Wird die Fernwartung von Externen durchgeführt, SOLLTEN alle Fernwartungsaktivitäten von internen Mitarbeitenden beobachtet werden. Alle Fernwartungsvorgänge durch Dritte SOLLTEN aufgezeichnet werden.

Mit externem Wartungspersonal MÜSSEN vertragliche Regelungen über die Sicherheit der betroffenen IT-Systeme und Informationen geschlossen werden. Die Pflichten und Kompetenzen des externen Wartungspersonals SOLLTEN in den vertraglichen Regelungen festgehalten werden.

Sollten Dienstleistende mehrere Kunden und Kundinnen fernwarten, MUSS gewährleistet sein, dass die Netze der Kunden und Kundinnen nicht miteinander verbunden werden. Die Fernwartungsschnittstellen SOLLTEN so konfiguriert sein, dass es Dienstleistenden nur möglich ist, auf die IT-Systeme und Netzsegmente zuzugreifen, die für seine Arbeit benötigt werden.

**OPS.1.2.5.A20 Betrieb der Fernwartung (S)**

Ein Meldeprozess für Support- und Fernwartungsanliegen SOLLTE etabliert werden.

Es SOLLTEN Mechanismen zur Erkennung und Abwehr von hochvolumigen Angriffen, TCP-State-Exhaustion-Angriffen und Angriffen auf Applikationsebene implementiert sein.

Alle Fernwartungsvorgänge SOLLTEN protokolliert werden.

#### OPS.1.2.5.A21 Erstellung eines Notfallplans für den Ausfall der Fernwartung (S)

Es SOLLTE ein Konzept entwickelt werden, wie die Folgen eines Ausfalls von Fernwartungskomponenten minimiert werden können. Dieses SOLLTE festhalten, wie im Falle eines Ausfalls zu reagieren ist. Durch den Notfallplan SOLLTE sichergestellt sein, dass Störungen, Schäden und Folgeschäden minimiert werden. Außerdem SOLLTE festgelegt werden, wie eine zeitnahe Wiederherstellung des Normalbetriebs erfolgen kann.

#### OPS.1.2.5.A24 Absicherung integrierter Fernwartungssysteme (S)

Bei der Beschaffung von neuen IT-Systemen SOLLTE geprüft werden, ob diese IT-Systeme oder einzelne Komponenten der IT-Systeme über Funktionen zur Fernwartung verfügen. Werden diese Funktionen nicht verwendet, SOLLTEN sie deaktiviert werden. Die Funktionen SOLLTEN ebenfalls deaktiviert werden, wenn sie durch bekannte Sicherheitslücken gefährdet sind.

Werden Fernwartungsfunktionen verwendet, die in die Firmware einzelner Komponenten integriert sind, SOLLTEN deren Funktionen und der Zugriff darauf so weit wie möglich eingeschränkt werden. Die Fernwartungsfunktionen SOLLTEN nur aus einem getrennten Managementnetz erreichbar sein.

#### OPS.1.2.5.A25 Entkopplung der Kommunikation bei der Fernwartung (S)

Direkte Fernwartungszugriffe von einem Fernwartungs-Client außerhalb der Managementnetze auf ein IT-System SOLLTEN vermieden werden. Ist ein solcher Zugriff notwendig, SOLLTE die Kommunikation entkoppelt werden. Dazu SOLLTEN Sprungserver verwendet werden. Der Zugriff auf Sprungserver SOLLTE nur von vertrauenswürdigen IT-Systemen aus möglich sein.

### 3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

#### OPS.1.2.5.A14 Dedizierte Clients und Konten bei der Fernwartung (H)

Zur Fernwartung SOLLTEN IT-Systeme eingesetzt werden, die ausschließlich zur Administration von anderen IT-Systemen dienen. Alle weiteren Funktionen auf diesen IT-Systemen SOLLTEN deaktiviert werden. Die Netzkommunikation der Administrationssysteme SOLLTE so eingeschränkt werden, dass nur Verbindungen zu IT-Systemen möglich sind, die administriert werden sollen.

Für Fernwartungszugänge SOLLTEN dedizierte Konten verwendet werden.

#### OPS.1.2.5.A22 Redundante Kommunikationsverbindungen (H)

Für Fernwartungszugänge SOLLTEN redundante Kommunikationsverbindungen eingerichtet werden. Die Institution SOLLTE Anbindungen zum Out-Of-Band-Management vorhalten.

#### OPS.1.2.5.A23 ENTFALLEN (H)

Diese Anforderung ist entfallen.

## 4. Weiterführende Informationen

### 4.1. Wissenswertes

Das Bundesamt für Sicherheit in der Informationstechnik beschreibt in seiner Veröffentlichung „Grundregeln zur Absicherung von Fernwartungszugängen“, wie Fernwartungszugänge sicher betrieben werden können.

Das Bundesamt für Sicherheit in der Informationstechnik beschreibt in seiner Veröffentlichung „Fernwartung im industriellen Umfeld“ wie Fernwartungszugänge im Industrieumfeld sicher betrieben werden können.